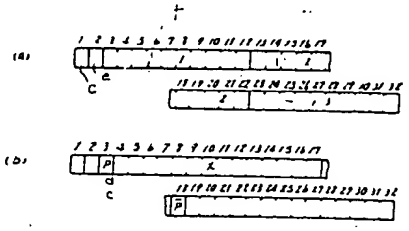
(54) DATA TRANSMISSION METHOD
(11) 3-169136 (A) (43) 22.7.1991 (19) JP
(21) Appl. No. 64-310218 (22) 28.11.1989
(71) OKI ELECTRIC IND CO LTD (72) TAKASHI TERAJIMA
(51) Int. Cl⁵. H04L1/00,H04J13/00

PURPOSE: To attain high performance data transmission by discriminating the parity at reception, handling a data in a frame as another information transmission data with less frequency of occurrence and sending another information transmission data without using a transmission bit in the substantial data transmission when a transmission error code is discriminated.

CONSTITUTION: A parity bit is added in a frame so as to be set as an even number (or odd number) parity at the transmission of a sampling transmission data and set to be an odd (even) parity in the case of transmission of another information transmission data. In this case of reception and of the discrimination of even (or odd) parity, the frame is processed as a frame handling a usual sampling transmission data, and in the case of discrimination of odd (or even) parity at the reception, the frame is processed as a frame handling another information transmission data with less frequency of occurrence. Thus, the data transmission is made highly sophisticated in the performance.

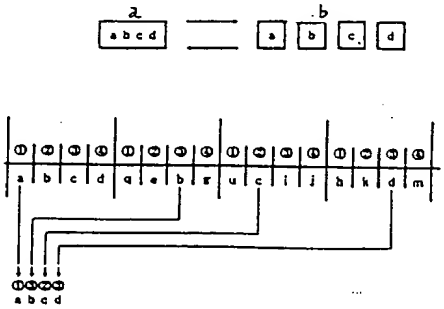


(a): at usual transmission, (b): at transmission of other information, c: synchronizing bit, d: parity bit (odd number), e: parity bit (even number), f: data

(54) CRYPTOGRAPHIC SYSTEM FOR ON-LINE SYSTEM
(11) 3-169137 (A) (43) 22.7.1991 (19) JP
(21) Appl. No. 64-310183 (22) 28.11.1989
(71) HOKURIKU NIPPON DENKI SOFTWARE K.K. (72) YUKIYASU SUMIO
(51) Int. Cl⁵. H04L9/00,G09C1/00,H04L9/10,H04L9/12

PURPOSE: To enhance the security of cryptography against interception of a specific channel in a digital communication line by decomposing a transmission text over plural channels ciphered in time series, sending the result and combining the texts into a reception text after the reception.

CONSTITUTION: In the case of data communication through a digital communication line, since an input information string is communicated through channels in time division, the string is divided into plural information strings. That is, an input information string "abcd" is divided into 4 information strings "a", "b", "c", "d". In the Figure a prescribed period is divided into 4 channels and the divided information strings "a", "b", "c", "d" are sent through the channels 1, 1, 1, 1 over the 4 periods, and in the case of reception, the information strings of channel numbers 1, 3, 2, 3 are extracted to combine the input information string of "abcd". Since the channel number used for the communication is not specific to each period, the channel number is used as time series cryptographic information in the communication system. Thus, intercept of a text is prevented.

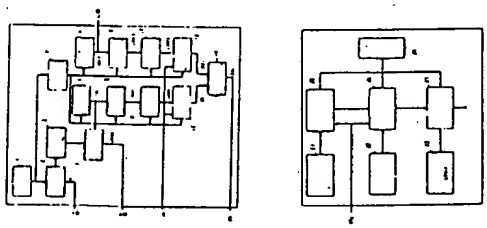


a: input information string, b: decomposed information strings

(54) KEY SHARING METHOD BASED ON IDENTIFICATION INFORMATION
(11) 3-169138 (A) (43) 22.7.1991 (19) JP
(21) Appl. No. 64-308679 (22) 28.11.1989
(71) MATSUSHITA ELECTRIC IND CO LTD (72) NATSUME MATSUZAKI(2)
(51) Int. Cl⁵. H04L9/06,G09C1/00,H04L9/14

PURPOSE: To prevent 1st and 2nd secret information sets from being acquired from a terminal equipment by using product of the 1st and 2nd secret information sets the secret information distributed to the terminal equipment.

CONSTITUTION: Let D1i be secret information of a terminal equipment, then the secret information at a terminal equipment is expressed as a linear combination between the secret information at the center and a public open value, and the secret information of the center is solved by conspiration of plural parties. When D2i is used as the secret information of a terminal equipment, a 3rd party terminal equipment (j) use its own secret information D2j and open public information sets E2i, E2j to obtain the value D2i being identical to the D2i in terms of modL from the relation of $D2i \times E2j = D2j \times D2i$:modL. Thus, the 3rd party uses the values obtained in this way in place of the secret information D2i of the regular terminal equipment thereby obtaining a common key among optional terminal equipments. However, in this case a D3i being the product is distributed as the secret information for terminal equipments. Thus, each of D1i, D2i cannot be acquired.



21: 1st open public value storage section, 22: 2nd open public value storage section, 23: secret information storage section, 25: multiplication residual arithmetic section, 26: 1st power residual arithmetic section, 27: 2nd power residual arithmetic section, kij: common key, 24: 3rd open public value storage section, 1: prime generating section, 2: N generating section, 3: g generating section, 7: power residual arithmetic section, 4: L generating section, 5: 1st e generating section, 6: 2nd e generating section, 8: 1st d generating section, 9: 2nd d generating section, 10: 1st V generating section, 11: 2nd V generating section, 12: 1st secret information generating section, 13: 2nd secret information generating section, 14: 3rd secret information generating section

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平3−169137

⑤1Int. Cl.⁵	識別記号	庁内整理番号	⑬公開 平成3年(1991)7月22日
H 04 L 9/00			
G 09 C 1/00		7343−5B	
H 04 L 9/10			
9/12			
		6914−5K H 04 L 9/00	Z

審査請求 未請求 請求項の数 1 (全7頁)

⑤4発明の名称　オンラインシステムの暗号化方式

⑳特　願 平1−310183
㉒出　願 平1(1989)11月28日

㉗発明者　角尾　幸保　石川県石川郡鶴来町安養寺1番地　北陸日本電気ソフトウエア株式会社内
㉑出願人　北陸日本電気ソフトウエア株式会社　石川県石川郡鶴来町安養寺1番地
㉔代理人　弁理士　内原　晋

明細書

発明の名称

オンラインシステムの暗号化方式

特許請求の範囲

通信回路を利用して電文を送受信するオンラインシステムの、送信側局である主局と受信側局である従局において、前記主局内の電文を入力してデジタル情報列に分解する電文分解手段と、

前記電文分解手段により引き渡された情報列を送信するためのチャネル選択をあらかじめ設定された時系列暗号化情報をもとに行う送信チャネル選択手段と、

前記従局内のデジタル通信回線を介して受信される電文の中から設定された時系列複号化情報をもとに受信チャネルをもとに受信チャネルを選択して情報列を取り出す受信チャネル選択手段と、

前記受信チャネル選択手段より引き取されるデジタル情報列を電文に合成し出力する電文合成手段とを含むことを特徴とするオンラインシステムの暗号化方式。

発明の詳細な説明

〔産業上の利用分野〕

本発明は、通信回線を利用したオンラインシステムと送信側局と受信側局とのセキュリティ技術に関し、特に情報通信時の電文の暗号強度を保証したオンラインシステムの暗号化方式に関する。

〔従来の技術〕

今日の社会では、航空便の座席予約などのプッシュホン・サービスをはじめとして、ファクシミリ・サービスやオンライン・バンキングなどのデジタル通信を使用したサービスが数多く利用されている。これらデジタル通信では、データの通信精度向上や通信容量増大にともなって、個人や企業にとどまらず社会全体にとっても重要なデータを扱う場合が多くなっている。このため、通信データの盗聴に対応する技術の確立が必要となってきている。従来、デジタル通信回線を利用してデ

ータを通信する場合は、一本の回線を複数のチャネルに時分割して情報を伝達するが、特定のチャネルを一回線として利用するために、通信データが周期的に通信されるのが一般的であった。すなわち第２図で示す、"ａｂｃｄ"という入力情報列を通信するために、"ａ"，"ｂ"，"ｃ"，"ｄ"の情報例に分解し、第３図に示すように周期ごとに時分割された同一の番号をもつチャネルを利用して情報列を通信するのが一般的であった。

〔発明が解決しようとする課題〕

上述した従来のデジタル通信回線の利用方式では、一つのチャネルが一つの回線に対応しているため電文が周期的に通信されることになり、チャネルが特定された場合には電文が容易に盗聴されるという欠点があった。

〔課題を解決するための手段〕

本発明は、通信回線を利用して電文を送受信するオンラインシステムの、送信側局である主局と受信側局である従局において、前記主局内の電文を入力してデジタル情報列に分解する電文分解手段と、前記電文分解手段より引き渡された情報列を送信するためのチャネル選択をあらかじめ設定された時系列暗号化情報をもとに行う送信チャネル選択手段と、前記従局内のデジタル通信回線を介して受信される電文の中からあらかじめ設定された時系列複号化情報をもとに受信チャネルを選択して情報列を取り出すチャネル選択手段と、前記受チャネル選択手段により引き渡されるデジタル情報列を電文に合成して出力する電文合成手段とを有している。

〔実施例〕

次に、本発明について図面を参照して説明する。

第１図は本発明の一実施例の概念図である。主局２は、電文１を取り込んで複数のデジタル情報列に分解する電文分解手段２１と、あらかじめ設定されている時系列暗号化情報を記憶する時系列暗号化情報記憶手段２３と、電文分解手段２１に接続され時系列暗号化情報をもとに送信チャネルを選択する送信チャネル選択手段２２と、送信チャネル選択手段２２とデジタル通信回線３に接続され送信チャネル選択手段２２によって指示されたチャネルよりデジタル通信回線３を介して情報列を送信する送信手段２４により構成される。

従局４はデジタル通信回線３に接続され主局２の情報列を受信する受信手段４１と、あらかじめ設定されている時系列複号化情報を記憶する時系列複号化記憶手段４３と、受信手段４１に接続され時系列複号化情報をもとに受信チャネルを選択する受信チャネル選択手段４２と、受信チャネル選択手段４２に接続され複数のデジタル情報列から電文５を合成する電文合成手段４４により構成される。

第２図、第３図、第４図はデジタル通信回線を使用した通信回線動作を説明する概念図であり、それぞれ、情報列の分割として合成動作、従来方式の通信動作、本実施例方式の通信動作の概念を示している。

第２図で示すように、デジタル通信回線によりデータを通信する場合は、入力情報列は時分割されチャネルを通して通信するために、複数の情報例に分割される。第２図では、入力情報列"ａｂｃｄ"を"ａ"，"ｂ"，"ｃ"，"ｄ"の四つの情報列に分割している。第３図で示すように、従来の方式によるデジタル通信動作では、引定期内の複数のチャネルに時分割し、その一定周期ごとにあられるチャネルを通して分割された情報列を送信し、また受信は特定チャネルの分割された情報列を順次取り出して入力情報列を合成した。第３図では、一定周期を４チャネルに分割し、その４周期期間に流ってそれぞれ①①①①のチャネルを通して"ａ"，"ｂ"，"ｃ"，"ｄ"の分解された情報列を送信し、受信はチャネル番号①①①①の情報列を取り出し、"ａｂｃｄ"の入力情報列を合成した例を示している。このようにして従来方式では、通信に使用すチャネル番号が周期ごとに特定しているので、チャネル番号を時系列非暗号化情報として通信方式といえる。

第４図で示すように、本実施例方式によるデジタル通信方式では、一定周期内の複数のチャネルに時分割し、複数チャネル番号にまたがったチャネルを通して分割された情報列を送信し、また受信は送信に使用されたチャネルの分割された情報列を順次取り出して入力情報を合成した。第４図では、一定周期を４チャネルに分割し、その４周期間に渡ってそれぞれ①①①①のチャネルを通して“ａ”，“ｂ”，“ｃ”，“ｄ”の分割された情報列を送信し、受信はチャネル番号①③②③の情報列を取り出し“ａｂｃｄ”の入力情報列を合成した例を示している。このように本実施例方式では、通信に使用するチャネル番号が周期ごとに特定しないので、チャネル番号を時系列暗号化情報とした通信方式といえる。

次に第５図を参照して本実施例の動作を説明する。

デジタル通信回線３を介して送信手段２４と受信手段４１の同期をとるために、主局２から通信開始指示を送信し（処理２－１）、従局４が通信開始指示を受了する（処理４－１）。主局は送信電文“ａｂｃｄ”を取り出し（処理２－２）、電文分解手段２１により電文を複数の情報列“ａ”に続く“ｂ”，“ｃ”，“ｄ”に分解する（処理２－３）。送信チャネル選択手段２２は時系列暗号化情報記憶手段より取り出した、時系列暗号化情報をもとに分解された情報列に対応させて送信するチャネルを選択する（処理２－４）。情報列は送信手段２４を通し、複数チャネルにまたがって暗号化されて従局へ送信される（処理２－５）。前記処理２－４，２－５を全情報列“ａ”に続く“ｂ”，“ｃ”，“ｄ”を終了するまで繰り返す（処理２－６）。従局４は、受信チャネル選択手段４２が時系列複号化情報記憶手段４３より取り出した時系列複号化情報をもとに送信チャネル選択手段２２と同期した受信チャネルを選択する（処理４－２）。受信手段４１は選択された受信チャネルに対応させて分解された情報列を受信する（処理４－３）。前記処理４－２，４－３を前情報列“ａ”に続く“ｂ”，“ｃ”，“ｄ”が終了するまで繰り返す（処理４－４）。電文合成手段４４は受信した全情報列より受信電文“ａｂｃｄ”を合成する（処理４－５）。従局４は受信電文“ａｂｃｄ”を取り出す（処理４－６）。主局２から通信終了指示を送信し（処理２－７）、従局４が通信終了指示を受了する（処理４－７）。

次に、本実施例の各手段の動作を説明する。

第６図は本実施例の電文分解手段の動作を示すフローチャートである。電文分解手段２１は一定の大きさの電文を取り出し（処理２１－１）、その電文をデジタル情報列に分解し（処理２１－２）、そのデジタル情報列を送信チャネル選択手段２２に引渡す（処理２１－３）。処理２１－１～－３を繰り返す。

第７図は本実施例の送信チャネル選択手段の動作を示すフローチャートである。送信チャネル選択手段２２は電文分解手段２１から情報列引渡を待つ（処理２２－１）。電文分解手段２１からの情報列引渡があった時、時系列暗号化情報記憶手段２３より時系列暗号化情報を取り出し（処理２２－２）、時系列暗号情報をもとに送信チャネルを選択し、（処理２２－３）、その選択チャネルを送信手段２４に指示し（処理２４－４）、送信デジタル情報列を送信手段２４に引き渡す（処理２２－５）。処理２２－２～－５を送信デジタル情報列が終了するまで繰り返す（処理２２－６）。処理２２－１～－６を繰り返す。

第８図は本実施例の送信手段の動作を示すフローチャートである。送信手段２４は入力通信開始指示かどうかを判断し（処理２４－２）、通信開始であれば通信開始を送信し（処理２４－１）、そうでなければ入力が通信終了指示かどうかを判断し（処理２４－３）、通信終了指示であれば通信終了し（処理２４－４）、そうでなければ入力がチャネル指示がどうかを判断し（処理２４－５）、チャネル支持であれば送信チャネルを変更し（処理２４－６）、そうでなければ情報列を送信する（処理２４－７）。

第９図は本実施例の受信手段の動作を示すフロ

ーチャートである．受信手段４１は入力が通信開始指示かどうかを判断し（処理４１－１）、通信開始であれば受信開始を受信チャネル選択手段４２に指示し（処理４１－２）、そうでなければ入力が通信終了指示かどうかを判断し（処理４１－３）、通信終了であれば受信終了を受信チャネル選択手段４２に指示し（処理４１－４）、そうでなければ受信チャネル選択手段４２に受信情報を引き渡す（処理４１－５）．

第１０図は本実施例の受信チャネル選択手段を示すフローチャートである．受信チャネル選択手段４２は受信手段４１からの受信開始指示を待つ（処理４２－１）．次に、受信手段４１からの受信終了指示があれば処理を終了し、なければ引渡情報列が在ると判断する（処理４２－２）．引渡情報列があった時、時系列複号化情報記憶手段４３より時系列複号化情報を取り出し（処理４２－３）、その時系列複号化情報をもとに受信チャネルを選択し（処理４２－４）、その受信チャネルよりデジタル情報列を取り出し（処理４２－５）、その情報列を電文合成手段４４に引き渡す（処理４２－６）．処理４２－２～４２－６を受信終了指示があるまで繰り返す．

第１１図は本実施例の電文合成手段の動作を示すフローチャートである．電文合成手段４４は受信チャネル選択手段４２から受け取り（処理４４－１）、そのデジタル情報列を電文に合成し（処理４４－２）、電文５を出力する（処理４４－３）．

〔発明の効果〕

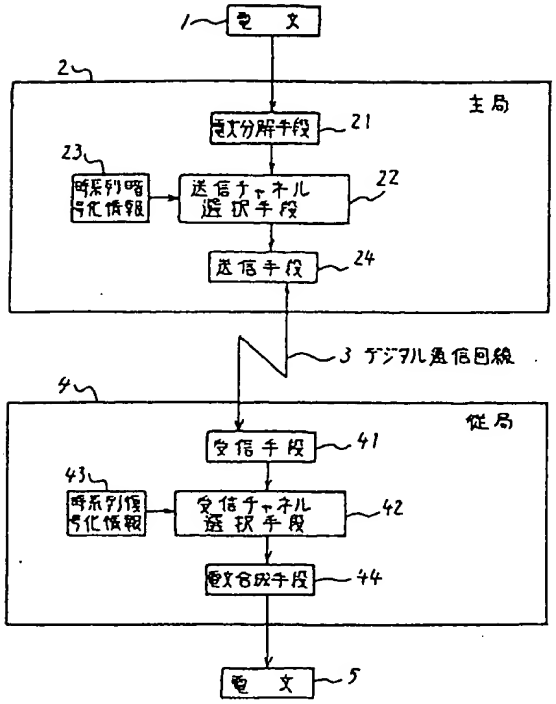
以上説明したように、本発明は時系列に暗号化された複数のチャネルにまたがって送信電文が分解されて送信され、受信後に受信電文に合成されるために、デジタル通信回線における特定チャネルの盗聴に対する暗号強度が高まる効果がある．

図面の簡単な説明

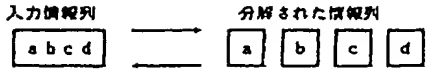
第１図は本発明の実施例を示すブロック図であり、第２図は情報列の分割と合成動作を説明する概念図であり、第３図は従来方式の通信動作を説明する概念図であり、第４図は本実施例方式の通信動作を説明する概念図である．第５図は本発明のフローチャートであり、第６図は電文分解手段の動作を示すフローチャートであり、第７図は送信チャネル選択手段の動作を示すフローチャートであり、第８図は送信手段の動作を示すフローチャートであり、第９図は受信手段の動作を示すフローチャートであり、第１０図は送信チャネル選択手段の動作を示すフローチャートであり、第１１図は電文合成手段の動作を示すフローチャートである．

１……送信電文、２……送信側局である主局、２１……電文をデジタル情報列に分解する電文分解手段、２２……送信するためのチャネル選択を行う送信チャネル選択手段、２３……あらかじめ設定されている時系列暗号化情報記憶手段、２４……送信手段、３……デジタル通信回路、４……受信側局である従局、４１…受信手段、４２……受信するためのチャネル選択を行う受信チャネル選択手段、４３……あらかじめ設定されている時系列複号化情報記憶手段、４４……デジタル情報列を電文に合成する電文合成手段、５……受信電文．

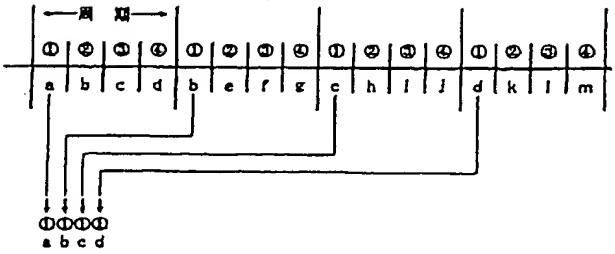
代理人　弁理士　内原　晋



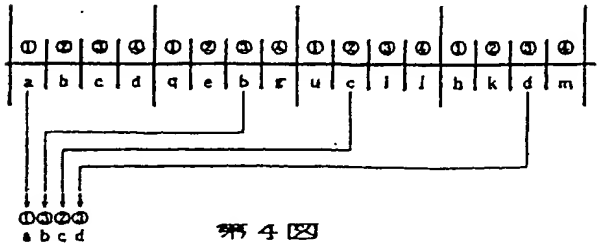
第 1 図



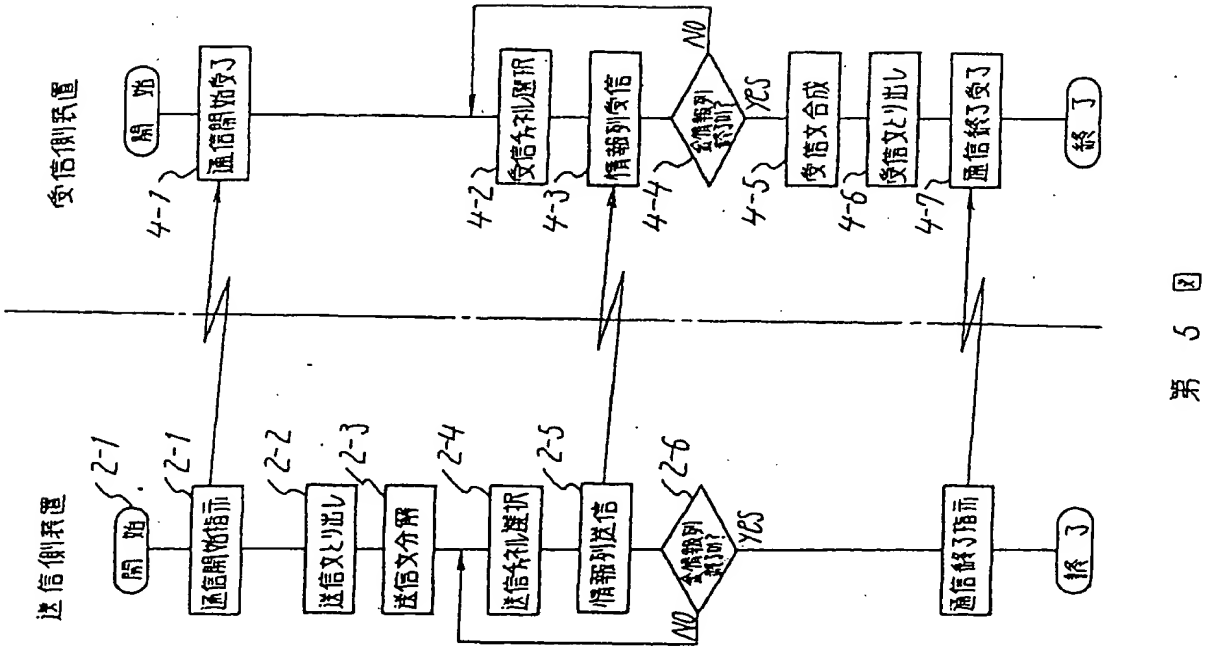
第 2 図



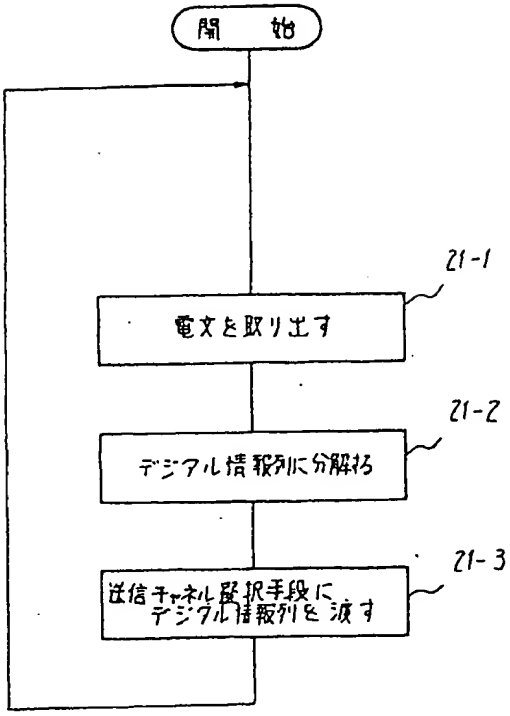
第 3 図



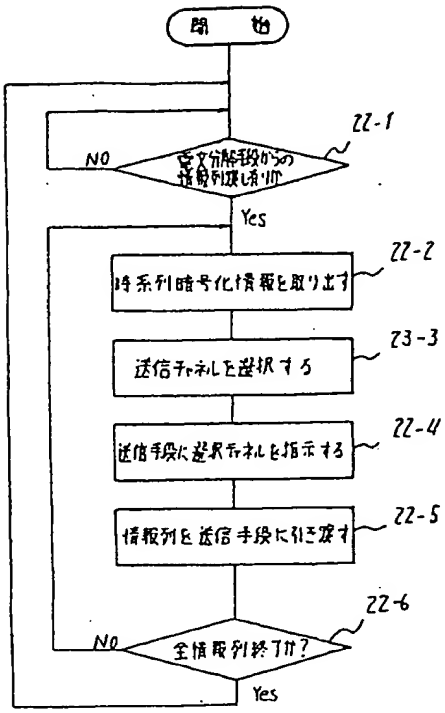
第 4 図



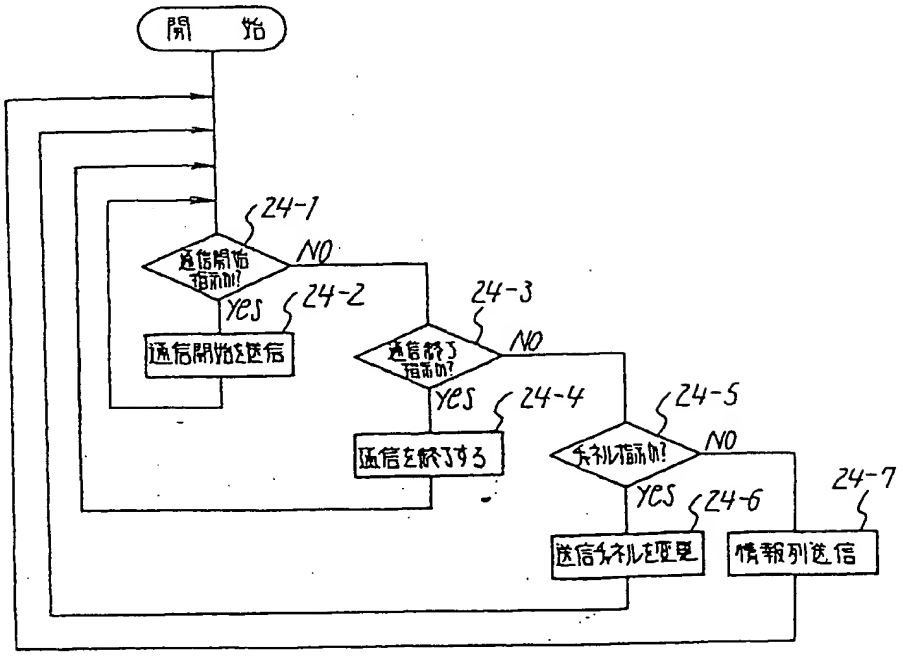
第 5 図


開　始
21-1
電文を取り出す
21-2
デジタル情報列に分解する
21-3
送信チャネル選択手段に
デジタル情報列を渡す

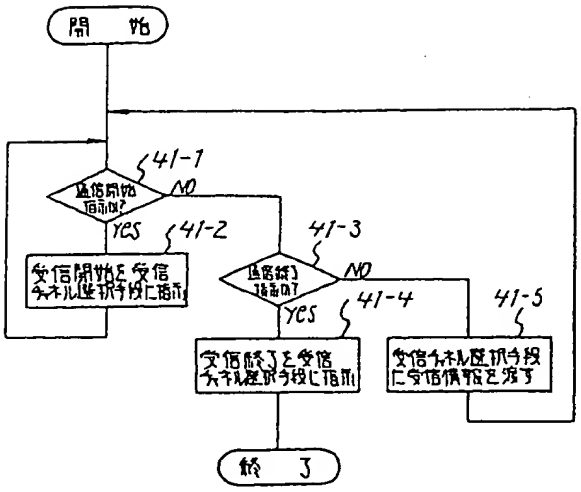
第　6　図


開　始
22-1
電文分解手段からの
情報列取り出し?
NO
Yes
22-2
時系列暗号化情報を取り出す
23-3
送信チャネルを選択する
22-4
送信手段に選択チャネルを指示する
22-5
情報列を送信手段に引き渡す
22-6
全情報列終了?
NO
Yes

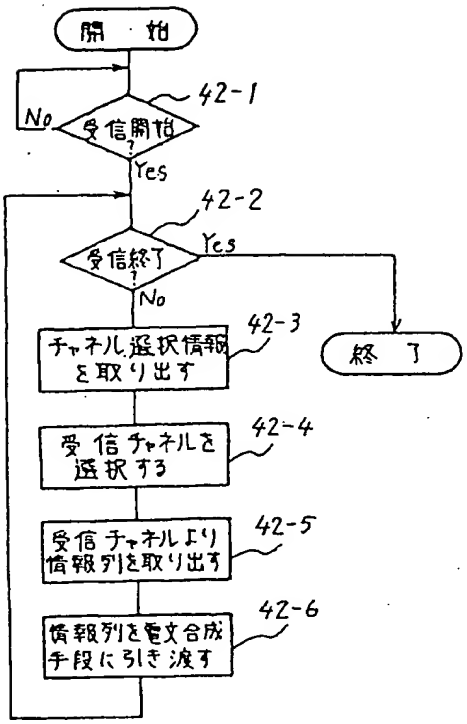
第　7　図


開　始
24-1
送信開始
指示?
NO
YES
24-2
通信開始を送信
24-3
送信終了
指示?
NO
YES
24-4
通信を終了する
24-5
チャネル指示?
NO
YES
24-6
送信チャネルを変更
24-7
情報列送信

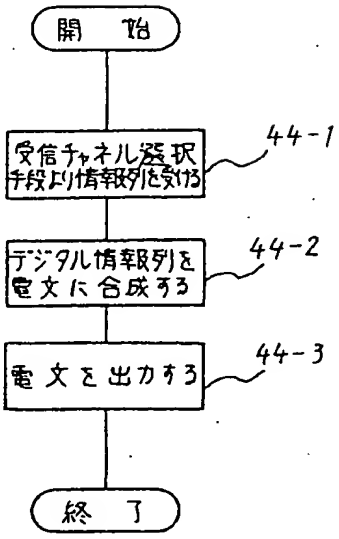
第　8　図



第　9　図



第　10　図



第　11　図